IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application : **10/507,190**

Applicant(s) : **TUYLS et al.**

Filed : **9/9/2004**

Confirmation : **1803**

T.C./Art Unit : **2109**

Examiner : **TRAORE, Fatoumata**

Atty. Docket : **NL-020192**

Title: **POLYNOMIAL-BASED MULTI-USER KEY GENERATION AND AUTHENTICATION METHOD AND SYSTEM**

Mail Stop: **APPEAL BRIEF - PATENTS**
Commissioner for Patents
Alexandria, VA 22313-1450

APPEAL UNDER 37 CFR 41.37

Sir:

This is an appeal from the decision of the Examiner dated 27 May 2008, finally rejecting claims 1-4 and 9-20 of the subject application.

This paper includes (each beginning on a separate sheet):

1. **Appeal Brief;**
2. **Claims Appendix;**
3. **Evidence Appendix; and**
4. **Related Proceedings Appendix.**

APPEAL BRIEF

I. REAL PARTY IN INTEREST

The above-identified application is assigned, in its entirety, to **Koninklijke Philips Electronics N. V.**

II. RELATED APPEALS AND INTERFERENCES

Appellant is not aware of any co-pending appeal or interference that will directly affect, or be directly affected by, or have any bearing on, the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-20 are pending in the application.

Claims 5-8 are objected to, but would be allowed if rewritten in independent form.

Claims 1-4 and 9-20 stand rejected by the Examiner under 35 U.S.C. 103(a).

These rejected claims are the subject of this appeal.

IV. STATUS OF AMENDMENTS

An amendment was filed on 10 July 2008, subsequent to the final rejection in the Office Action dated 27 May 2008.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The invention provides a method and system for increasing the number of users/devices that may share a 'global secret'. Each authorized device receives a particular device secret based on the global secret (page 2, lines 26-30). Due to the structure of the global secret and device secrets, any two devices having device secrets that are based on the same global secret can generate a common secret (page 2, lines 17-25). If the device secrets are not based on the same global secret, the generated secrets at each device will differ; therefore, this generation of a common secret certifies that both devices are based on the same global secret (page 1, lines 14-23). In an embodiment of this invention, the global secret includes two symmetric polynomials in two variables ($P(x,y)=P(y,x)$ and $Q(x,y)=Q(y,x)$), and each device secret includes a value of one variable of each of the symmetric polynomials (p and q) and the coefficients of the product of the polynominals when the polynomial is fixed with these values of the polynomials ($P_p(y)=P(x,y|x=p)$ and $Q_q(y)=Q(x,y|x=q)$). If two devices exchange their fixed values (p1,q1 and p2,q2), each device can generate a secret: $P_{p1}(p2)*Q_{q1}(q2)$ at the device receiving p2 and q2, and $P_{p2}(p1)*Q_{q2}(q1)$ at the device that receives p1 and q1. Because the global secret polynomials are symmetric, $P_{p1}(p2) = P_{p2}(p1)$ and $Q_{q1}(q2)=Q_{q2}(q1)$; that is, $P(x,y|x=p1,y=p2) = P(x,y|x=p2,y=p1)$ and $Q(x,y|x=q1,y=q2) = Q(x,y|x=q2,y=q1)$. Therefore, if both device secrets are based on the same global secret $P(x,y)$ and $Q(x,y)$, the determined secrets, $P_{p1}(p2)*Q_{q1}(q2)$ and $P_{p2}(p1)*Q_{q2}(q1)$, will be equal (page 3, lines 17-21). To further enhance the security of this technique, the parameters q1 and q2 may each also be multiplied by a random variable r1 and r2, and the products r1q1 and r2q2 are exchanged (page 3, lines 27-29; FIG. 4).

As claimed in independent claim 1, the invention comprises a method of generating a common secret between a first party and a second party, in which the first party holds a value p_1 and a symmetrical polynomial $P(x,y)$ fixed in the first argument by the value p_1, and the first party performs the steps of sending the value p_1 to the second party, receiving a value p_2 from the second party and calculating the common secret S_1 by evaluating the polynomial $P(p_1, y)$ in p_2 (page 2, lines 26-30; FIG. 1), characterized in that the first party additionally holds a value q_1 and a symmetrical polynomial $Q(x, z)$ fixed in the first argument by the value q_1, and further performs the steps of sending q_1 to the second party, receiving a value q_2 from the second party and calculating the secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$ (page 3, lines 17-21).

As claimed in independent claim 16, the invention comprises a system comprising a first party, a second party and a trusted third party, that is arranged to generate a common secret between the first party and the second party, in which the first party holds a value p_1 and a symmetrical polynomial $P(x,y)$ fixed in the first argument by the value p_1, and the first party performs the steps of sending the value p_1 to the second party, receiving a value p_2 from the second party and calculating the common secret S_1 by evaluating the polynomial $P(p_1, y)$ in p_2 (page 2, lines 26-30; FIG. 1),

wherein the first party additionally holds a value q_1 and a symmetrical polynomial $Q(x, z)$ fixed in the first argument by the value q_1, and further performs the steps of sending q_1 to the second party, receiving a value q_2 from the second party and calculating the secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$ (page 3, lines 17-21).

As claimed in independent claim 17, the invention comprises a device (prover P in FIG. 4) arranged to:

hold a value p_1, a symmetrical polynomial P(x,y) fixed in the first argument by the value p_1, a value q_1, and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q_1 (page 9, lines 14-22; FIG. 4),

send the value p_1 to a second party (verifier V),

receive a value p_2 from the second party (page 10, line 8),

evaluate the polynomial $P(p_1, y)$ in p_2 (page 10, lines 8-9; FIG. 1),

send q_1 to the second party,

receiving a value q_2 from the second party (page 10, line 8),

evaluate the polynomial $Q(q_1, q_2)$ (page 10, lines 8-9), and

calculate a secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$ (page 10, line 15; page 3, lines 20-21).

As claimed in independent claim 19, the invention comprises a computer readable media that includes a program product for causing one or more processors to generate a common secret between a first party and a second party, in which the first party holds a value p_1 and a symmetrical polynomial P(x,y) fixed in the first argument by the value p_1, and the first party performs the steps of sending the value p_1 to the second party, receiving a value p_2 from the second party and calculating the common secret S_1 by evaluating the polynomial $P(p_1, y)$ in p_2 (page 2, lines 26-30; FIG. 1),

wherein the first party additionally holds a value q_1 and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q_1, and further performs the steps of sending q_1 to the second party, receiving a value q_2 from the second party and calculating the secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$ (page 3, lines 17-21).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 9-12, and 16-19 stand rejected under 35 U.S.C. 103(a) over Leighton et al. (USP 5,519,778, hereinafter Leighton) and Hoffstein et al. (USP 6,076,163, hereinafter Hoffstein.

Claims 2, 3, 4, and 20 stand rejected under 35 U.S.C. 103(a) over Leighton, Hoffstein, and Matyas et al. (USP 5,953,420, hereinafter Matyas).

Claims 13-15 stand rejected under 35 U.S.C. 103(a) over Leighton, Hoffstein, and Menezes et al. (Handbook of Applied Cryptography, hereinafter Menenzes).

VII. ARGUMENT

Claims 1, 9-12, and 16-19 stand rejected under 35 U.S.C. 103(a) over Leighton and Hoffstein

Claims 1, 9-12, and 16-19

The combination of Leighton and Hoffstein fails to teach or suggest a method for generating a common secret as a product of two symmetric polynomials, as specially claimed in claim 1, upon which claims 2-15 depend. Independent claims 16, 17, and 19 include similar features.

The Office action acknowledges that Leighton fails to teach receiving a second value (q2) from a second party and calculating a secret as S1=Q(q1,q2)*P(p1,p2) (Office action, page 5, lines 17-19), and asserts that Hoffstein provides this teaching. The applicants respectfully disagrees with this assertion.

The Office action asserts that Hoffstein teaches determining a secret as the product of two symmetric polynomials at FIG. 3 and column 3, lines 31-46. At the cited text, Hoffstein teaches:

> "The above-described user identification technique can be converted to a digital signature technique by the prover applying a one-way hash function to $A_g(x)$ and a message m to generate a simulated challenge polynomial c(x) which may be used in conjunction with g(x) and f(x) to generate the response polynomial h(x). The verifier receives m, $A_g(x)$ and h(x), uses the one-way hash function to derive c(x), and compares $A_h(x)$ to $A_g(x)*(A_f(x)+A_c(x))$ in order to authenticate the digital signature of the prover. Alternatively, the signature might consist of c(x) and h(x). From this $A_g(x)$ can be recovered as $A_h(x)*(A_f(x)+A_c(x))-1$ and the hash of this quantity and the message m can be compared to the polynomial c(x). A desired security level in both the user identification and digital signature techniques may be provided by selecting appropriate constraints for the polynomials g(x), c(x) and h(x)." (Hoffstein, column 3, lines 31-46.)

As is clearly evident, in the cited text, Hoffstein does not address generating a common secret, does not address symmetric polynomials, does not address receiving a value (q1) for determining the value of a polynomial Q(q1,q2), and specifically does not address receiving a value q_2 from a second party and calculating a secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$, as specifically claimed in claim 1.

The Office action fails to identify where Hoffstein teaches receiving a value (q2) that is an argument to a polynomial (Q(q1,q2)), other than to state "(Fig. 3)" (Office action, page 5, last line). At Fig. 3, Hoffstein clearly illustrates the transfer of polynomials ($A_g(x)$, c(x), and h(x)) between a "prover" and "verifier", and not a particular argument (q2) of a polynomial (Q(q1,q2)). As is well known in the art, and as taught by Hoffstein and the applicants, a polynomial is transferred by communicating the coefficients of the polynomial, or communicating information from which the coefficients can be determined. As evidenced by steps (5) and (6) in Fig. 3 of Hoffstein, the purpose of transferring the polynomials (and not an argument to be used to determine a particular value of the polynomial), is to verify the determined range of the coefficients of the polynomial. Nowhere in Fig. 3, or in the description of Fig. 3, does Hoffstein teach determining the value of any of the polynomials based on a given value of an argument, to determine a secret.

Additionally, nowhere in Fig. 3, or in the description of Fig. 3, does Hoffstein teach that any of the polynomials are symmetric polynomials. To the contrary, all of Hoffstein's polynomials are polynomials in one variable. As is well known in the art, a symmetric polynomial must include at least two variables, because the definition of symmetric is that reversing the order of the arguments has no effect on the determined value of the polynomial (Q(x,y)=Q(y,x)):

> "In mathematics, a symmetric polynomial is a polynomial $P(X_1, X_2, \ldots, X_n)$ in n variables, such that if any of the variables are interchanged, one obtains the same polynomial. Formally, P is a *symmetric polynomial*, if for any permutation σ of the subscripts 1, 2, ..., n one has $P(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}) = P(X_1, X_2, \ldots, X_n)$." (http://en.wikipedia.org.)

An example of a symmetric polynomial is Q(x,y) = x*y; reversing the order of the arguments has no effect on the value of the polynomial. A polynomial in one variable cannot be said to be "symmetric", because there is no other variable to "interchange" with the single variable to establish symmetry. A "symmetric polynomial in one variable" is a meaningless term; such a polynomial cannot exist using the well-established definition of a symmetric polynomial.

In response to the applicants' argument that Hoffstein fails to teach the use of symmetric polynomials to generate a secret (key), the Examiner references Hoffstein's figures 1A and 1B (Examiner's Answer, page 2, fifth paragraph). The applicants respectfully note that Hoffstein's figures 1A and 1B fail to address polynomials, and specifically do not address symmetric polynomials. In Hoffstein's figure 1A, Hoffstein teaches that "Prover's private key is a mod q, public key is $v=\alpha^{-a}$ mod p." The applicants respectfully note that neither of these terms is a polynomial; figure 1B includes similar modulo functions to define the keys, and not polynomials.

Throughout the Office action, the Examiner appears to equate the use of a symmetric algorithm with the use of symmetric polynomials. The two are not equivalent, and, in most cases, are not related. A symmetric algorithm as used in the field of cryptography refers to the use of the same key at both the encryption device and the decryption device. A symmetric polynomial, on the other hand, is a mathematical term that refers to the fact that each argument of the polynomial has the same effect on the value of the polynomial, and is substantially independent of

the field of cryptography. Symmetric keys do not, per se, rely on or imply the use of symmetric polynomials, and the use of symmetric keys does not suggest or imply the use of the product of two symmetric polynomials, as claimed by the applicants.

Because the combination of Leighton and Hoffstein fails to teach or suggest receiving two parameter values (p2,q2) and determining a secret that is a product of the value of two symmetric polynomials based on these values (P(p1,p2)*Q(q1,q2)), as specifically claimed in claim 1, and because the Office action fails to identify where Hoffstein teaches symmetric polynomials, and a secret based on a product of two symmetric polynomials, the applicants respectfully maintain that the rejection of claims 1 and 9-12 under 35 U.S.C. 103(a) over Leighton and Hoffstein is unfounded, and should be reversed by the Board.

Claims 2-4 and 20 stand rejected under 35 U.S.C. 103(a) over Leighton, Hoffstein and Matyas.

Claims 2-4 and 20

Claims 2-4 are dependent upon claim 1, and claim 20 is dependent upon claim 16. In this rejection, the Office action relies on the combination of Leighton and Hoffstein for teaching the elements of claims 1 and 16.

As noted above, the combination of Leighton and Hoffstein fails to teach or suggest the elements of claims 1 and 16. Accordingly, the applicants respectfully maintain that the rejection of claims 2-4 and 20 under 35 U.S.C. 103(a) that relies on Leighton and Hoffstein for teaching the elements of claims 1 and 16 is unfounded, and should be reversed by the Board.

Claims 13-15 stand rejected under 35 U.S.C. 103(a) over Leighton, Hoffstein and Menenzes.

Claims 13-15

Claims 13-15 are dependent upon claim 1, and in this rejection, the Office action relies on the combination of Leighton and Hoffstein for teaching the elements of claim 1.

As noted above, the combination of Leighton and Hoffstein fails to teach or suggest the elements of claim 1. Accordingly, the applicants respectfully maintain that the rejection of claims 13-15 under 35 U.S.C. 103(a) that relies on Leighton and Hoffstein for teaching the elements of claim 1 is unfounded, and should be reversed by the Board.

CONCLUSIONS

Because the combination of Leighton and Hoffstein fails to teach or suggest receiving two parameter values (p2,q2) and determining a secret that is a product of the value of two symmetric polynomials based on these values (P(p1,p2)*Q(q1,q2)), as claimed in each of the applicants' independent claims, the applicants respectfully request that the Examiner's rejection of claims 1-4 and 9-20 under 35 U.S.C. 103(a) be reversed by the Board, and the claims be allowed to pass to issue.

Respectfully submitted

/Robert M. McDermott/
Robert M. McDermott, Attorney
Registration Number 41,508
patents@lawyer.com
804-493-0707

Please direct all correspondence to:
Corporate Counsel
U.S. PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001

CLAIMS APPENDIX

1. A method of generating a common secret between a first party and a second party, in which the first party holds a value p_1 and a symmetrical polynomial P(x,y) fixed in the first argument by the value p_1, and the first party performs the steps of sending the value p_1 to the second party, receiving a value p_2 from the second party and calculating the common secret S_1 by evaluating the polynomial $P(p_1, y)$ in p_2, characterized in that the first party additionally holds a value q_1 and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q_1, and further performs the steps of sending q_1 to the second party, receiving a value q_2 from the second party and calculating the secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$.

2. The method of claim 1, in which the first party further performs the steps of obtaining a random number r_1, calculating $r_1 \cdot q_1$, sending $r_1 \cdot q_1$ to the second party, receiving $r_2 \cdot q_2$ from the second party and calculating the secret S_1 as $S_1=Q(q_1, r_1 \cdot r_2 \cdot q_2)\cdot P(p_1, p_2)$.

3. The method of claim 2, in which the first party holds the value q_1 multiplied by an arbitrarily chosen value r, and the product $Q(q_1, z)P(p_1, y)$ instead of the individual polynomials $P(p_1, y)$ and $Q(q_1, z)$, and the first party performs the steps of calculating $r_1 \cdot r \cdot q_1$, sending $r_1 \cdot r \cdot q_1$ to the second party, receiving $r_2 \cdot r \cdot q_2$ from the second party and calculating the secret S_1 as $S_1=Q(q_1, r_1 \cdot r_2 \cdot r \cdot q_2)\cdot P(p_1, p_2)$.

4. The method of claim 1, in which the second party holds a value p_2 and a value q_2, the symmetrical polynomial P(x, y) fixed in the first argument by the value p_2, the symmetrical polynomial Q(x, z) fixed in the first argument by the value q_2, and the second party performs the steps of sending q_2 to the first party, receiving q_1 from the first party and calculating a secret S_2 as $S_2=Q(q_2, q_1)\cdot P(p_2, p_1)$, whereby the common secret has been generated if the secret S_2 equals the secret S_1.

5. The method of claim 1, in which a trusted third party performs the steps of choosing a symmetric (n+1) × (n+1) matrix T, constructing the polynomial P using entries from the matrix T as respective coefficients of the polynomial P, constructing the polynomial Q(x, y), choosing the value p_1, the value p_2, the value q_1 and the value q_2, sending the value p_1, the value q_1, the polynomial P(x, y) fixed in the first argument by the value p_1 and the polynomial Q(x, z) fixed in the first argument by the value q_1 to the first party, and sending the value p_2, the value q_2, the polynomial P(x, y) fixed in the first argument by the value p_2 and the polynomial Q(x, z) fixed in the first argument by the value q_2 to the second party

6. The method of claim 5, in which the trusted third party further arbitrarily chooses a value r, sends the value $r \cdot q_1$ instead of the value q_1 and the product $Q(q_1, z)P(p_1, y)$ instead of the individual polynomials $P(p_1, y)$ and $Q(q_1, z)$ to the first party and sends the value $r \cdot q_2$ instead of the value q_2 and the product $Q(q_2, z)P(p_2, y)$ instead of the individual polynomials $P(p_2, y)$ and $Q(q_2, z)$ to the second party.

7. The method of claim 5, in which the trusted third party further performs the steps of

choosing a set comprising *m* values p_i, including the values p_1 and p_2,

calculating a space **A** from the tensor products $\vec{p}_i^{\,V} \otimes \vec{p}_j^{\,V}$ of the Vandermonde vectors $\vec{p}_i^{\,V}$ built from the set of values p_i,

choosing a vector $\vec{\gamma}_1$ and a vector $\vec{\gamma}_2$ from the perpendicular space $\mathbf{A}^{\perp}$ of the space **A**, constructing a matrix $T_{\Gamma_1} = T+\Gamma_1$ from the vector $\vec{\gamma}_1$ and a matrix $T_{\Gamma_2} = T+\Gamma_2$ from the vector $\vec{\gamma}_2$, constructing a polynomial $P^{\Gamma_1}(x, y)$ using entries from the matrix T_{Γ_1} and sending the polynomial $P^{\Gamma_1}(x, y)$ fixed in the first argument by the value p_1 to the first party, and

constructing a polynomial $P^{\Gamma_2}(x, y)$ using entries from the matrix T_{Γ_2} and sending the polynomial $P^{\Gamma_2}(x, y)$ fixed in the first argument by the value p_2 to the second party.

8. The method of claim 5, in which a number *m'* of values p_i, and *m'* < *m*, are distributed to additional parties.

9. The method of claim 1, in which the first party and the second party use a non-linear function on the generated secret S1 and S2, respectively, before using it as a secret key in further communications.

10. The method of claim 9 in which a one-way hash function is applied to the generated secrets S1 and S2.

11. The method of claim 9 in which a non-linear function in the form of a polynomial is applied to the generated secrets S1 and S2.

12. The method of claim 1, further comprising the step of verifying that the second party knows the secret S_1.

13. The method of claim 12, in which the first party subsequently applies a zero-knowledge protocol to verify that the second party knows the secret S_1.

14. The method of claim 12, in which the first party subsequently applies a commitment-based protocol to verify that the second party knows the secret S_1.

15. The method of claim 14, in which the second party uses a symmetric cipher to encrypt a random challenge, and sends the encrypted random challenge to the first party and the first party subsequently uses the same symmetric cipher as a commit function to commit himself to a decryption of the encrypted random challenge.

16. A system comprising a first party, a second party and a trusted third party, that is arranged to generate a common secret between the first party and the second party, in which the first party holds a value p_1 and a symmetrical polynomial P(x,y) fixed in the first argument by the value p_1, and the first party performs the steps of sending the value p_1 to the second party, receiving a value p_2 from the second party and calculating the common secret S_1 by evaluating the polynomial $P(p_1, y)$ in p_2,

wherein the first party additionally holds a value q_1 and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q_1, and further performs the steps of sending q_1 to the second party, receiving a value q_2 from the second party and calculating the secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$.

17. A device (P) arranged to:

hold a value p_1, a symmetrical polynomial P(x,y) fixed in the first argument by the value p_1, a value q_1, and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q_1,

send the value p_1 to a second party,

receive a value p_2 from the second party,

evaluate the polynomial $P(p_1, y)$ in p_2,

send q_1 to the second party,

receiving a value q_2 from the second party,

evaluate the polynomial $Q(q_1, q_2)$, and

calculate a secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$.

18. The device of claim 17, comprising storage means for storing the polynomial P and the polynomial Q in the form of their respective coefficients.

19. A computer readable media that includes a program product for causing one or more processors to generate a common secret between a first party and a second party, in which the first party holds a value p_1 and a symmetrical polynomial P(x,y) fixed in the first argument by the value p_1, and the first party performs the steps of sending the value p_1 to the second party, receiving a value p_2 from the second party and calculating the common secret S_1 by evaluating the polynomial $P(p_1, y)$ in p_2,

wherein the first party additionally holds a value q_1 and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q_1, and further performs the steps of sending q_1 to the second party, receiving a value q_2 from the second party and calculating the secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$.

20. The system of claim 16, wherein the second party holds a value p_2 and a value q_2, the symmetrical polynomial P(x, y) fixed in the first argument by the value p_2, the symmetrical polynomial Q(x, z) fixed in the first argument by the value q_2, and the second party performs the steps of sending q_2 to the first party, receiving q_1 from the first party and calculating a secret S_2 as $S_2=Q(q_2, q_1)\cdot P(p_2, p_1)$, whereby the common secret has been generated if the secret S_2 equals the secret S_1.

EVIDENCE APPENDIX

No evidence has been submitted that is relied upon by the appellant in this appeal.

RELATED PROCEEDINGS APPENDIX

Appellant is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have any bearing on the Board's decision in the pending appeal.